DRAFT — prepared without legal advice — must be reviewed by a qualified solicitor before use

Strata Data Processing Addendum

Version 2026-10-03-draft
Effective 2026-10-03
Provider Racelogic Limited (company no. 02743719)

In plain terms. When a business streams through Strata, the footage and its run data can contain personal data that the business controls. This addendum is the contract under Article 28 of the UK GDPR and the EU GDPR that governs how we process that data for you: only on your instructions, securely, with sub-processors you can see in advance, and deleted when you ask or when your retention period ends.

1. Scope and parties

1. This Data Processing Addendum ("**DPA**") forms part of the Terms of Service between Racelogic Limited ("**Racelogic**", the **processor**) and the business customer that has accepted them ("**Customer**", the **controller**). It applies automatically to every business customer and needs no signature. A countersigned copy is available on request from `legal@strata.stream`.
2. It applies to personal data that Racelogic processes on the Customer's behalf in providing Strata ("**Customer Personal Data**"), as described in Annex I. It does not apply to personal data Racelogic processes as a controller, such as account and billing data, which the Privacy Policy covers.
3. "**Data Protection Law**" means the UK GDPR, the Data Protection Act 2018, the EU GDPR (Regulation (EU) 2016/679) and any national law implementing or supplementing them, as they apply to the processing. Terms such as **controller**, **processor**, **personal data**, **personal data breach** and **data subject** have the meanings given in Data Protection Law.
4. If this DPA conflicts with the Terms of Service, this DPA prevails as to the processing of Customer Personal Data.

2. Racelogic's obligations

Racelogic will:

1. **Instructions.** Process Customer Personal Data only on the Customer's documented instructions, including with regard to international transfers, unless required to do otherwise by UK or EU law, in which case Racelogic will inform the Customer before processing unless that law forbids it. The Terms of Service, this DPA, and the Customer's use and configuration of Strata (for example its destinations, recording setting and retention period) are the Customer's complete instructions. Racelogic will tell the Customer if it believes an instruction infringes Data Protection Law.
2. **Confidentiality.** Ensure that every person it authorises to process Customer Personal Data is under a duty of confidentiality.
3. **Security.** Implement the technical and organisational measures in Annex II, and keep them appropriate to the risk. Racelogic may change them, provided the overall level of protection is not reduced.
4. **Sub-processors.** Engage sub-processors only as set out in section 3.
5. **Data subject requests.** Taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures to respond to requests from data subjects. Strata's self-

service export and deletion tools are the primary means of assistance. Racelogic will pass to the Customer, without responding itself, any request it receives that relates to Customer Personal Data.

6. **Assistance.** Assist the Customer, taking into account the information available to Racelogic, with its obligations on security, personal data breach notification, data protection impact assessments and prior consultation with supervisory authorities.
7. **Personal data breaches.** Notify the Customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data. The notice will describe, as far as then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, its likely consequences, and the measures taken or proposed. Racelogic will provide further information as it becomes available. Notice is sent to the organisation's admins by email.
8. **Deletion and return.** At the end of the provision of Strata, or when the Customer deletes its organisation, delete Customer Personal Data, unless UK or EU law requires it to be kept. Before then, the Customer can download its recordings and export its organisation's data from the dashboard at any time. Deleted data remains in encrypted backups until they are overwritten, within 35 days.
9. **Audits.** Make available to the Customer the information necessary to demonstrate compliance with Article 28, and allow for and contribute to audits, including inspections, by the Customer or an auditor it mandates. The Customer will first ask for the information in writing; if an audit is still needed, it will give at least 30 days' notice, carry it out during business hours without disrupting Racelogic's operations, bind its auditor to confidentiality, and bear its own costs.

3. Sub-processors

1. The Customer gives Racelogic general authorisation to engage sub-processors. The current list is in Annex III and at Sub-processors.
2. Racelogic will give at least 30 days' notice of any intended addition or replacement, by updating Sub-processors and emailing the organisation's admins. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may terminate its subscription and receive a refund of fees prepaid for the period after termination.
3. Racelogic will impose on each sub-processor, by written contract, data protection obligations that offer at least the same protection as this DPA, and remains liable to the Customer for each sub-processor's performance of them.

4. International transfers

1. Racelogic is in the United Kingdom, and processes Customer Personal Data in the UK and the European Economic Area. Where a transfer of Customer Personal Data to a sub-processor outside the UK and EEA is not covered by adequacy regulations or an adequacy decision, Racelogic will make it under an appropriate safeguard: the EU–US Data Privacy Framework (and its UK Extension) where the recipient is certified, or otherwise the EU Standard Contractual Clauses with the UK Addendum, or the UK International Data Transfer Agreement.
2. Where the Customer is in the EEA, the transfer of Customer Personal Data from the Customer to Racelogic in the UK relies on the European Commission's adequacy decision for the UK. [To be completed: counsel to confirm the fallback (EU SCCs Module 2) should that decision lapse]

DRAFT — prepared without legal advice — must be reviewed by a qualified solicitor before use

5. The Customer's obligations

1. The Customer is responsible for having a lawful basis for the processing it instructs, for giving any notices and obtaining any consents required (for example from people who appear in its footage), and for the accuracy of its instructions.
2. The Customer is responsible for choosing the recording setting and retention period appropriate to its purposes.

6. Liability and duration

1. Each party's liability under this DPA is subject to the limitations in the Terms of Service, except where Data Protection Law does not allow it.
2. This DPA lasts for as long as Racelogic processes Customer Personal Data.

Annex I — Details of the processing

Item	Details
Controller	The Customer: the business organisation that accepted the Terms of Service contact through its admins
Processor	Racelogic Limited, Unit 10, Swan Business Centre, Osier Way, Buckingham, MK18 1TB, United Kingdom. Contact: `privacy@strata.stream`
Subject matter	Providing Strata: bonded live video transport, recording, delivery and analysis
Duration	The term of the Customer's use of Strata, and then until deletion as described in section 2
Nature and purpose	Receiving, reassembling, transcoding, recording, storing, analysing and delivering the Customer's live streams to the destinations it configures; showing live previews and recordings in the dashboard; keeping run telemetry and logs so the Customer can see how its streams performed
Categories of data subjects	People who appear in or are heard in the Customer's footage; the Customer's staff and contractors who operate its encoders; anyone else whose personal data the Customer chooses to include
Categories of personal data	Images and voices in video and audio; any names, text or other information visible or audible in the footage; device and network data in run telemetry and logs (IP addresses, mobile network operator, cell identifiers that may indicate approximate location)
Special category data	Not intended. Footage may incidentally reveal special category data (for example health or religious belief) if the Customer films it; the Customer is responsible for having a lawful basis
Frequency	Continuous, while the Customer streams
Retention	Recordings and run data: the Customer's retention period (the plan's maximum of 7, 30, 90 or 365 days, or shorter as the Customer chooses), or none while recording is off. Packet captures: 7 days at most. Encrypted backups: 35 days

DRAFT — prepared without legal advice — must be reviewed by a qualified solicitor before use

Annex II — Technical and organisational measures

Area	Measures
Encryption in transit	The website, dashboard and API are served only over TLS. Encoders and receivers connect to the control plane over TLS-protected WebSockets
Stream encryption	Every stream started through Strata gets its own randomly generated key. Each media datagram between encoder and receiver is encrypted and authenticated with ChaCha20-Poly1305, under keys derived from that stream key with HKDF-SHA256. A datagram that fails authentication is discarded
Secrets at rest	Destination stream keys, per-stream media keys and YouTube access tokens are sealed in the database with ChaCha20-Poly1305 under keys held outside the database
Authentication	Passwords are hashed with Argon2id. Sign-in failures are slowed down per account and per address. Session and email-link tokens are stored only as hashes; email links are single-use and expire (24 hours for verification, 1 hour for password reset, and a reset signs out every session). The session cookie is HttpOnly and SameSite
Device identity	Each encoder and receiver enrols with its own Ed25519 key pair, and must prove possession of the private key to connect
Tenant separation	Every organisation's devices, destinations, streams and recordings are scoped to that organisation, and every request is checked against the user's membership and role (admin, operator or viewer)
Staff access	No interface gives Racelogic staff access to customers' footage, recordings, runs or devices. Staff tooling is limited to account and subscription administration, and every staff action is recorded in the audit log. Staff status cannot be granted through the product
Server access	Administrative access to servers is limited to named Racelogic engineers, by SSH key only (password sign-in is disabled), and hosts run a restrictive firewall
Logging and audit	Security-relevant actions are recorded in an audit log kept for 12 months and visible to the people concerned. Server logs are kept for 30 days
Backups and resilience	The database is backed up regularly; backups are encrypted with `age` before they leave the server and kept for 35 days
Retention and deletion	Recordings and run data are deleted automatically at the end of the Customer's retention period. Customers can delete individual runs, all recordings, or the whole organisation at any time
Software assurance	Every change is tested automatically before release; dependencies are checked for known vulnerabilities and for licence compliance on every change
Hosting	Servers are hosted by the sub-processors in Annex III in professionally managed data centres with physical access control [To be completed: confirm the hosting providers' certifications (for example ISO/IEC 27001) for each data centre used]

DRAFT — prepared without legal advice — must be reviewed by a qualified solicitor before use

Annex III — Sub-processors

Racelogic uses the following sub-processors. The "Footage" column shows which of them may process Customer Personal Data in footage and run data. The current list is always at Sub-processors.

Provider	What it does	Where	Footage	Transfer safeguard
Hetzner Online GmbH	Hosting: the control plane, database, receivers, recordings and backups	Germany and Finland	Yes	None needed: processed in the EEA, which UK law recognises as adequate
Google Cloud EMEA Limited (Google Cloud Platform)	Hosting, replacing Hetzner after a planned migration [To be completed: migration date; give 30 days' notice before it starts]	United Kingdom (London region)	Yes	Processed in the UK. Any access from the US by Google LLC: EU–US Data Privacy Framework and UK Extension
Cloudflare, Inc.	DNS for strata.stream, and forwarding of email sent to our strata.stream addresses [To be completed: confirm whether Cloudflare also proxies web traffic]	United States and Cloudflare's global network	No	EU–US Data Privacy Framework and UK Extension
Amazon Web Services EMEA SARL (Amazon SES)	Sending service emails (verification, password reset, invitations, usage and account notices)	United Kingdom (London region)	No	Processed in the UK. Any access from the US by Amazon.com, Inc.: EU–US Data Privacy Framework and UK Extension
[To be completed: Racelogic's email provider]	The mailbox that receives email sent to our strata.stream addresses	[To be completed: location]	No	[To be completed: safeguard]

Racelogic Limited, a company registered in England and Wales under company number 02743719. Registered office: Unit 10, Swan Business Centre, Osier Way, Buckingham, MK18 1TB, United Kingdom. VAT number: [To be completed: UK VAT registration number].